SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

Software Assurance Forum for Excellence in Code

Directions for Effective Product Security Assessment

Eric Baize
Senior Director, Product Security Office
EMC Corporation
Eric.Baize@emc.com

September 2012

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

About SAFECode

The Software Assurance Forum for Excellence in Code (SAFECode) is a global, industry-led effort to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services

www.safecode.org

Juniper NETWORKS

SAP®

Microsoft®

SIEMENS

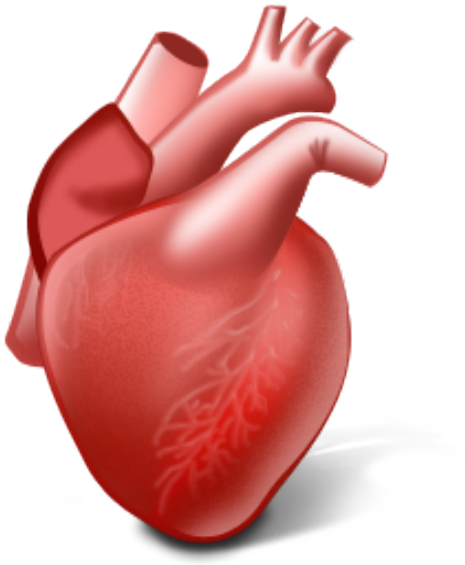
NOKIA

symantec™

Adobe®

The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.

Learning from Science



How can you best evaluate the risk of a person to die from heart disease?

Method #1: Demand a Declaration

“I, _____ _______, solemnly declare that I will not die from a heart attack”

Method #2: Perform a Lab Test

- Point in time measurement
- Partial and incomplete
- Can be tricked

Measure blood pressure and cholesterol

Method #3: Assess Lifestyle & Preparedness

✓

Activities that maintain blood pressure and cholesterol low

Ability to respond quickly and efficiently

Assessing Product Security

How can you best evaluate the risk that an IT product might contain a software vulnerability?

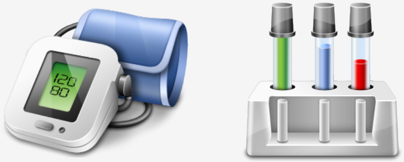
Three Methods for Assessing the Security of an IT Product

1

“I, _____ _______,
solemnly declare that I have no vulnerability in my product”

Demand a vendor declaration

2



Test the product

3

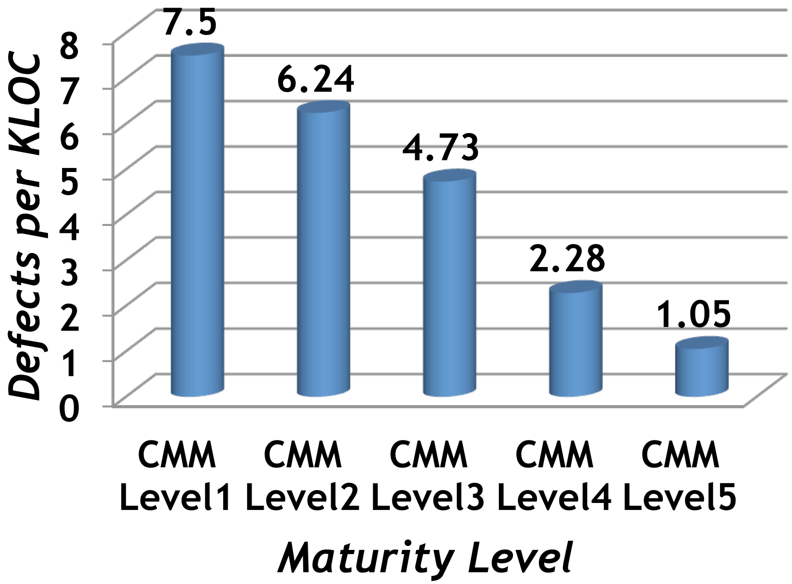
Assess vendor’s security processes

SAFECode Software Assurance Forum for Excellence in Code Driving Security and Integrity

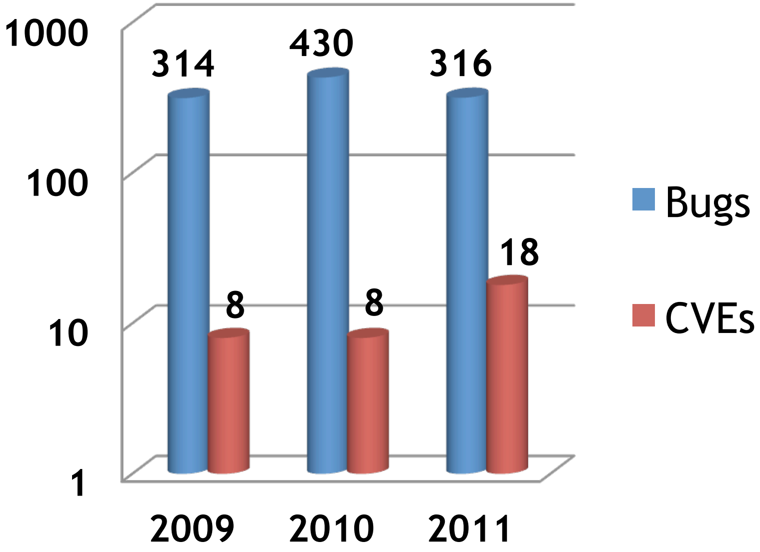
Assessing Product Security

1 Demand a vendor “no vulnerability“ declaration

Software Defect Density & Organization Maturity (SEI)



Confirmed bugs and CVEs for Apache Tomcat (log. scale)



Real software does have defects …

… some of which are vulnerabilities

2 Test or evaluate the product

Independent software security assessment

- Independent consultant / tool based assessment
- Point in time indicator dependent on the skills of the tester
- Partial and incomplete: Limited insights without access to internal design and source code
- Does not predict preparedness to unknown vulnerabilities.

Third party evaluations

- Current evaluations focus more on security capabilities than process
- No agreed upon international framework for evaluating secure software development process

Published vulnerability rate

- Unreliable measurement of the process outcome
- Greatly dependent on ease of access to product

3 Assess Vendor's Security Process ✓

Start with the vendor's public information:

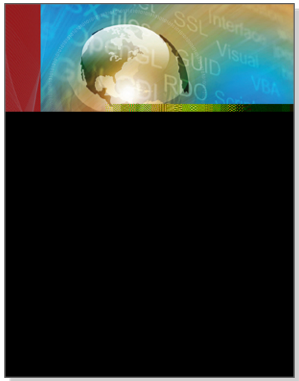
- Does the organization developing the product have secure software development standards in place?
- Do they publicly share their software assurance practices?
- Do they have a team with authority that provides the necessary oversight?
- Are developers properly trained to develop secure software?
- Do they have an easy to find way to report vulnerabilities on their product?
- Do they have a process in place to properly and expeditiously address reported vulnerabilities?

Secure Development Practices

Fundamental Practices for Secure Software Development - Second Edition

- **Focus:** Provide a foundational set of secure development practices based on an analysis of the real-world actions of SAFECode members

- **Key Objectives:** Help others initiate or improve their own software security programs and encourage the industry-wide adoption of fundamental secure development methods.



New: Practical Security Stories and Security Tasks for Agile Development Environments (July 2012)

Summary

- Software products will always contain vulnerabilities, no credible vendor will attest to the contrary.
- Tool-based assessment or vulnerability counts are point in time, subjective and incomplete
- Understanding a vendor secure software development process is the best predictor of the security of its product
  - Start with simple assessment of documented practices
  - New evaluation initiatives focus on vendor's process
    - Open Group's *Open Trusted Technology Provider Standard*
    - ISO 27034-1 Application Security – Overview and Concepts
  - SAFECode will continue to document proven vendor practices for secure software development that can serve as a reference

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

www.safecode.org
Twitter: @safecodeforum
Blog: http://blog.safecode.org

Eric Baize
Senior Director, Product Security Office
EMC Corporation
Eric.Baize@emc.com